JACKSON
PUBLIC SCHOOLS
Transforming lives through excellent education

RFP 2026-02-27

Advanced Email and Collaboration Security Solution

Issue Date: Friday, August 28, 2026

Submission Deadline: Thursday, September 17, 2026

Time: 10:00 a.m. (Central Standard Time)

Office at 601-973-8582 for assistance. Questions regarding proposal specifications are to be addressed to the Project Administrator listed in the proposal.

I. Invitation

II. Procurement Schedule (Tentative)

III. RFP Coordinator / Point of Contact

IV: Submission

V. Legal and Administrative Requirements

- **A. Public Records**
- **B. Ethics / Conflict of Interest**
- **C. E-Verify**
- **D. Availability of Funds / Non-Appropriation**
- **E. Insurance**
- **F. Term and Termination**

VI. Introduction and Background

- **A. Scope of Work**
- **B. Minimum Technical Response**
- **C. Performance Specifications**
- **D. Vendor Specifications**
- **E. Proposal Submission Requirements**
- **F. Evaluation Criteria**
- **G. Pricing Requirements**

VII. General Information

- **A. Specifications and Technical Requirements**

VII. Proposal Format and Required Contents

- **Exhibit E-1: Proposal Form and Signature Page**
- **Exhibit E-2: Submission Cover Sheet and Configuration Summary**
- **Exhibit E-3: Assurances and Signature Form**

I. Invitation

Jackson Public School District (JPSD) is soliciting proposals from qualified vendors for goods and/or services as described in this RFP. All products and services must meet the specifications or be approved equivalents.

The selected proposer shall provide the Services described below. Proposals must clearly explain how the proposer will meet each requirement.

II. Procurement Schedule (Tentative)

The District anticipates the following schedule. The District reserves the right to modify this schedule at any time.

Bid Issued	Friday, August 28, 2026
~~Prebid Meeting (virtual)~~	-
Deadline for Written Questions	Wednesday, September 9, 2026
District Issues Responses/Addenda	Monday, September 14, 2026
Proposal Submission Deadline	Thursday, September 17, 2026, 10:00 A.M.
Evaluation Period	
~~Optional Presentations/Demos~~	-
Notice of Intent to Award (anticipated)	
Board Approval	
Contract Start Date (anticipated)	

III. Bid Coordinator / Point of Contact

Communications regarding this RFP must be submitted in writing to the designated RFP coordinator designated below:

- Name: Michele Mays
- Title: Procurement Supervisor
- Email: rfp@jackson.k12.ms.us
- Phone: 601-973-8582

Proposers shall not contact other District employees, Board members, or representatives regarding this RFP during the procurement process.

IV. Proposal Instructions and Requirements

Please be advised that Jackson Public Schools will accept electronic proposal submissions only for this solicitation. Printed, mailed, or hand-delivered proposals will not be accepted or considered.

Proposals must be submitted electronically through Central Bidding at the link below: www.centralbidding.com

Vendors are responsible for ensuring proposals are successfully uploaded and submitted prior to the deadline.

Important Submission Notes

- The Proposal Submission Deadline is Thursday, September 17, at 10:00 a.m. Central time, as stated in Section II - Procurement Schedule.
- Late proposals will not be opened or considered.
- Faxed or emailed proposals will not be accepted.
- The District is not responsible for technical issues related to electronic submission.
- Vendors are encouraged to submit proposals early to ensure timely reception.

Proposal Format Requirements

- Proposal Cover Page must be the first page
- Proposal must be signed by an authorized official
- Incomplete proposals will not be evaluated

Pricing Requirements (if applicable)

- All prices must be net and include all applicable discounts
- Unit pricing prevails in case of discrepancies
- Prices must be rounded to two (2) decimal places
- Freight and shipping costs must be included, if applicable

Payment Terms (If applicable)

- Payment issued after satisfactory delivery or completion of services
- No partial payments unless specified
- Multi-year and open purchase orders follow contracted schedules

Insurance Requirements

The Contractor shall maintain the following insurance coverage for the duration of the contract:

- Commercial General Liability
  Contractors must maintain a minimum of $1,000,000 in General Liability coverage.
  Jackson Public Schools (JPS) must be listed as an Additional Insured on this policy. Coverage shall be primary and non-contributory.
- Workers' Compensation
  Any Contractor or subcontractor entering JPS school campuses, administrative buildings, or

project sites must maintain Workers' Compensation insurance with a minimum limit of $1,000,000.

- Certificate Holder Requirement
  Jackson Public Schools must be listed as the Certificate Holder on all Certificates of Insurance (COIs). COIs must be provided to JPS prior to commencing any work or entering District property.

Evaluation and Award

- Award will be made to the responsive and responsible proposer whose proposal is determined to be most advantageous to the District (best value), considering price and other evaluation factors stated in this RFP.
- Evaluation may include, as applicable: price, compliance with RFP requirements, responsiveness/completeness, references, and overall value.
- All awards are subject to approval by the Board of Trustees and availability of funds.
- The District reserves the right to reject any or all proposals, waive informalities and minor irregularities, and take any action in the District's best interest consistent with applicable Mississippi law.
- The District may request clarification, verify information, and contact references.
- Optional demonstrations/presentations:
  - The District may invite the highest-ranked proposers to participate in demonstrations, presentations, or clarification meetings.
  - Invitation is at the District's discretion and does not guarantee award.
  - Demonstrations must address the proposer's platform, enrollment tools, reporting, and other features relevant to this RFP. Failure to participate when requested may result in disqualification.
- The District may negotiate with one or more proposers, as permitted, to obtain the best value for the District.

Performance, Default, and Termination

Failure to perform in accordance with the contract may result in termination and the vendor being held responsible for any excess costs incurred by the District.

Guarantees and Warranties

All goods and services must meet the specifications outlined in this RFP. Non-conforming goods or services must be replaced at the vendor's expense.

Addenda

Vendors must acknowledge receipt of all addenda issued during the RFP process and submit any required additional information with their proposal.

Important Notices

- All proposal contents become public records after award/notice of intent, subject to the Mississippi Public Records Act and applicable exemptions.
- The District reserves the right to reject any and all proposals, waive informalities, and negotiate with the selected proposer in the District's best interest.

- Proposers are responsible for reviewing the entire RFP and submitting all required forms and attachments.

  All question and answers will be posted on the **Google** document link:

  https://docs.google.com/document/d/1lXNGplxhPDZL-mJJ9sp9BB85fKeC6xolvZJC5LDJJes/edit?usp=sharing

- Questions regarding this RFP must be submitted in writing to George Slade, Executive Director of Information Technology Services, by September 09, 2026. Questions and answers material to all bidders will be distributed to all vendors who have indicated intent to respond, consistent with open and fair competitive bidding practice.

VI. Introduction and Background

Jackson Public School District ("the District") is issuing this Request for Proposal (RFP) to solicit competitive proposals from qualified vendors for an advanced email and collaboration security solution. The District is the third-largest public school district in Mississippi, serving approximately 17,000 students and employing nearly 3,500 staff across 35 schools.

The District's productivity and communication environment is built on Microsoft 365, which includes native email filtering capabilities. The District recognizes that phishing remains a leading entry point for ransomware and other cyberattacks against K-12 institutions nationally, and that native, single-layer email filtering alone is frequently insufficient against modern, AI-assisted social engineering and account takeover attempts. The District further recognizes its obligation to protect sensitive student data under the Family Educational Rights and Privacy Act (FERPA) as that data moves through email, chat, and file-sharing channels used by staff.

The District intends to procure a solution that supplements its existing Microsoft 365 environment with an additional, independent layer of threat detection and data protection, without displacing or requiring removal of its existing Microsoft licensing investment.

This RFP is intended to be vendor-neutral and describes the District's required capabilities in functional terms. No specific manufacturer, product, or brand is intended to be favored. Any product, feature name, or specification referenced herein should be read as illustrative of the required capability, and proposals for equivalent solutions meeting the stated functional requirements will be evaluated on equal footing.

A. Purpose and Scope of Work

The District seeks proposals for a solution (or combination of licensed products and implementation services from a single responsible vendor) that provides:

- Advanced threat detection for email delivered through the District's Microsoft 365 tenant.
- Extended protection for collaboration and file-sharing applications used by District staff.
- Data loss prevention capabilities covering sensitive student and staff data.
- Reduced administrative and incident-response burden on the District's IT staff.
- Implementation, configuration, administrator training, and ongoing technical support for the life of the contract term.

The awarded solution must integrate with the District's existing Microsoft 365 environment without requiring the removal of native Microsoft security tooling and without requiring changes to the District's mail exchanger (MX) records or core mail-flow routing.

B. Minimum Technical Requirements

Proposals must address each requirement below and indicate compliance using the Compliance Matrix in Appendix A. Requirements marked (M) are mandatory; a proposal that does not meet a mandatory requirement, or does not clearly demonstrate an equivalent capability, may be deemed non-responsive.

3.1 Deployment and Architecture

3.1.1 The solution must integrate with Microsoft 365 via a supported application programming interface (API) or equivalent method that does not require changing the District's MX records or rerouting mail flow through a third-party gateway. (M)

3.1.2 The solution must be capable of being deployed and operational within days, not months, of contract execution. (M)

3.1.3 The solution must operate as a supplemental layer alongside the District's existing Microsoft 365 security tools without requiring their removal. (M)

3.1.4 The solution must support the District's current Microsoft 365 licensing tier(s) without requiring an upgrade to a higher Microsoft license tier as a precondition of functioning.

3.2 Threat Detection and Prevention

3.2.1 The solution must use multiple, independent, AI/machine-learning-based detection engines rather than relying solely on static signature or reputation-based filtering. (M)

3.2.2 The solution must continuously re-evaluate messages and links after initial delivery, not only at the point of arrival, to catch threats that weaponize after delivery (e.g., delayed-detonation phishing links). (M)

3.2.3 The solution must demonstrate, through independent third-party testing, published performance data, or verifiable customer references, a phishing detection effectiveness rate of at least 99% and a malware detection effectiveness rate of at least 99%. (M)

3.2.4 The solution must detect and flag business email compromise (BEC) attempts, including executive impersonation and vendor/invoice fraud patterns, using behavioral and content analysis rather than sender-domain blocklists alone.

3.3 Internal Threat and Account Takeover Protection

3.3.1 The solution must scan internal-to-internal email traffic (i.e., messages between District staff mailboxes), not only inbound/outbound mail crossing the network perimeter, to detect lateral phishing originating from a compromised internal account. (M)

3.3.2 The solution must include an anomaly-detection capability that monitors account logins and flags suspicious authentication activity indicative of account takeover.

3.3.3 The solution must provide a mechanism to automatically or semi-automatically contain a compromised account (e.g., session revocation, alerting, or quarantine) pending administrator review.

3.4 Data Loss Prevention (DLP)

3.4.1 The solution must provide data loss prevention capabilities that identify and control the transmission of sensitive data, including personally identifiable student information subject to FERPA. (M)

3.4.2 DLP policies must be able to be applied consistently across email and, where applicable, collaboration/file-sharing channels covered under Section 3.5, rather than being limited to email alone.

3.4.3 The solution must allow District administrators to define, test, and modify DLP policies without requiring vendor professional services for routine policy changes.

3.5 Collaboration Platform Security

3.5.1 The solution must extend threat detection, malicious file sandboxing, and data loss prevention coverage to Microsoft Teams. (M)

3.5.2 The solution must support extension of equivalent protections to SharePoint Online and OneDrive for Business.

3.5.3 The solution should support extension of equivalent protections to additional collaboration and file-sharing platforms (e.g., Slack, Google Workspace, or third-party file-sharing services) in the event the District adopts them during the contract term.

3.5.4 Malicious file detection within collaboration platforms must include automated sandboxing/detonation of files prior to a user being able to open or download them.

3.6 Administration, Reporting, and SOC Support

3.6.1 The solution must provide a centralized administrative console with role-based access for District IT staff.

3.6.2 The solution must provide reporting sufficient to demonstrate a measurable reduction in the volume of malicious or unwanted email reaching end-user inboxes, to support the District's limited IT staffing capacity.

3.6.3 Vendor must describe available managed detection/response or incident-response support options, including any incident response service that can be engaged in the event of a confirmed compromise.

3.7 Optional / Value-Added Capabilities

The District will give favorable consideration, but does not require, proposals that also include the following at an identified incremental cost:

3.7.1 Domain-based Message Authentication, Reporting and Conformance (DMARC) monitoring and enforcement assistance.

3.7.2 Ongoing, simulated phishing exercises and security awareness training for District staff.

3.7.3 Monitoring for District staff or student-facing credentials appearing in known data-breach or dark-web sources.

3.7.4 Email archiving sufficient to support public records requests and litigation hold requirements applicable to a Mississippi public school district.

3.8 Compliance and Data Privacy

3.8.1 Vendor must describe how the proposed solution supports the District's obligations under FERPA with respect to student personally identifiable information. (M)

3.8.2 Vendor must describe data encryption practices for data at rest and in transit.

3.8.3 Vendor must disclose where covered data is hosted/processed and describe any subcontractor or sub-processor relationships involved in service delivery.

3.8.4 Vendor must provide evidence of an independent security attestation (e.g., SOC 2 Type II or equivalent) covering the proposed service.

C. Performance Specifications

1. **API-based, non-MX-record deployment architecture** — "Solution must integrate directly via API with Microsoft 365/Google Workspace without requiring MX record changes or inline mail flow modification, and must be capable of deploying within 24–48 hours without disruption to existing mail routing."

2. **Minimum measurable catch rate for phishing and malware, independently validated** — "Solution must demonstrate a phishing catch rate of at least 99% and malware catch rate validated by an independent third-party testing lab (e.g., NSS Labs, AV-Comparatives, or equivalent)."

3. **Post-delivery remediation / retroactive quarantine capability** — "Solution must be able to detect and remove malicious emails from user inboxes after delivery, including messages already opened by the recipient, without requiring end-user action."

4. **AI/ML-driven behavioral and contextual analysis (not signature-based alone)** — "Solution must use machine learning models analyzing sender behavior, language patterns, historical trust relationships, and header/domain anomalies to detect zero-day and social-engineering-based attacks (BEC, impersonation, display-name spoofing) in addition to signature/reputation-based filtering."

5. **Unified collaboration-suite coverage under a single license/console** — "Solution must extend threat protection and DLP beyond email to at least Teams, SharePoint, OneDrive, and one additional third-party collaboration platform (e.g., Slack, Google Drive), managed from a single administrative console

D. Vendor Qualifications

Proposals must include the following information about the proposing vendor and, if applicable, its implementation partner:

- Company background, years in operation, and financial stability sufficient to support a multi-year public-sector contract.
- Evidence of experience serving K-12 school districts of comparable or larger size, including at least three (3) verifiable references from education-sector customers within the last 24 months.
- Evidence of independent industry analyst recognition (e.g., a named Leader or comparable top-tier ranking in a recognized analyst evaluation of email security solutions published within the past 24 months).
- Description of the support model, including support hours, escalation procedures, and named account management for the District.
- Disclosure of any subcontracted implementation, support, or managed-service partner who will be performing work under this contract, including that partner's relevant qualifications.

E. Proposal Submission Requirements

Proposals must be organized in the following format and submitted by the deadline identified on the cover page. Late proposals will not be considered.

1. Cover Letter — signed by an individual authorized to bind the vendor.
2. Executive Summary — a brief, non-technical summary of the proposed solution.
3. Technical Response — a point-by-point response to each requirement in Section 3, using the Compliance Matrix in Appendix A.
4. Vendor Qualifications — responsive to Section 4.
5. Implementation Plan — proposed timeline, milestones, and staffing for deployment.
6. Pricing Proposal — responsive to Section G, submitted as a separate, clearly labeled section or attachment.
7. Contract / License Agreement — a copy of the vendor's standard terms proposed to govern the engagement.

Questions regarding this RFP must be submitted in writing to George Slade, Executive Director of Information Technology Services, by September 09, 2026 . Questions and answers material to all bidders will be distributed to all vendors who have indicated intent to respond, consistent with open and fair competitive bidding practice.

F. Evaluation Criteria

Proposals will be evaluated using the weighted criteria below. The District reserves the right to request oral presentations, product demonstrations, or a proof-of-concept/pilot deployment prior to final award.

Criterion	Weight
Compliance with mandatory technical requirements (Section 3)	35%
Overall technical capability and value-added features	20%
Vendor qualifications, K-12 references, and support model	15%
Implementation plan and timeline	10%
Total cost of ownership over contract term (Section 7)	20%

G. Pricing Requirements

Vendors must propose pricing on a per-mailbox/per-user, per-year basis, inclusive of all licensing, support, and any managed services included in the base proposal. Pricing must be presented for:

- A 3-year term, invoiced annually (with any multi-year discount clearly identified).
- Optional add-on capabilities identified in Section 3.7, priced separately.
- One-time implementation/onboarding fees, if any, itemized separately from recurring licensing costs.

Pricing must remain firm for a minimum of 90 days following the proposal due date.

Appendix A: Technical Compliance Matrix

Vendors must complete this matrix in full. For each requirement, indicate Full Compliance, Partial Compliance, or No Compliance, and provide a brief explanation or reference to the section of the technical response where the capability is described.

Ref.	Requirement	Compliance (Full/Partial/No)	Reference / Notes
3.1.1	The solution must integrate with Microsoft 365 via a supported application programming interface (API) or equivalent method that does not require changing the District's MX records or rerouting mail flow through a third-party gateway. (M)		
3.1.2	The solution must be capable of being deployed and operational within days, not months, of contract execution. (M)		
3.1.3	The solution must operate as a supplemental layer alongside the District's existing Microsoft 365 security tools without requiring their removal. (M)		
3.1.4	The solution must support the District's current Microsoft 365 licensing tier(s) without requiring an upgrade to a higher Microsoft license tier as a precondition of functioning.		
3.2.1	The solution must use multiple, independent, AI/machine-learning-based detection engines rather than relying solely on static signature or reputation-based filtering. (M)		
3.2.2	The solution must continuously re-evaluate messages and links after initial delivery, not only at the point of arrival, to catch threats that weaponize after delivery (e.g., delayed-detonation phishing links). (M)		
3.2.3	The solution must demonstrate, through independent third-party testing, published performance data, or verifiable customer references, a phishing detection effectiveness rate of at least 99% and a malware detection effectiveness rate of at least 99%. (M)		
3.2.4	The solution must detect and flag business email compromise (BEC) attempts, including executive impersonation and vendor/invoice fraud patterns, using behavioral and content analysis rather than sender-domain blocklists alone.		
3.3.1	The solution must scan internal-to-internal email traffic (i.e., messages between District staff mailboxes), not only inbound/outbound mail crossing the network perimeter, to detect lateral phishing originating from a compromised internal account. (M)		
3.3.2	The solution must include an anomaly-detection capability that monitors account logins and flags suspicious authentication activity indicative of account takeover.		
3.3.3	The solution must provide a mechanism to automatically or semi-automatically contain a compromised account (e.g., session revocation, alerting, or quarantine) pending administrator review.		
3.4.1	The solution must provide data loss prevention capabilities that identify and control the transmission of sensitive data, including personally identifiable student information subject to FERPA. (M)		
3.4.2	DLP policies must be able to be applied consistently across email and, where applicable, collaboration/file-sharing channels covered under Section 3.5, rather than being limited to email alone.		
3.4.3	The solution must allow District administrators to define, test, and modify DLP policies without requiring vendor professional services for routine policy changes.		
3.5.1	The solution must extend threat detection, malicious file sandboxing, and data loss prevention coverage to Microsoft Teams. (M)		
3.5.2	The solution must support extension of equivalent protections to SharePoint Online and OneDrive for Business.		

3.5.3	The solution should support extension of equivalent protections to additional collaboration and file-sharing platforms (e.g., Slack, Google Workspace, or third-party file-sharing services) in the event the District adopts them during the contract term.		
3.5.4	Malicious file detection within collaboration platforms must include automated sandboxing/detonation of files prior to a user being able to open or download them.		
3.6.1	The solution must provide a centralized administrative console with role-based access for District IT staff.		
3.6.2	The solution must provide reporting sufficient to demonstrate a measurable reduction in the volume of malicious or unwanted email reaching end-user inboxes, to support the District's limited IT staffing capacity.		
3.6.3	Vendor must describe available managed detection/response or incident-response support options, including any incident response service that can be engaged in the event of a confirmed compromise.		
3.7.1	Domain-based Message Authentication, Reporting and Conformance (DMARC) monitoring and enforcement assistance.		
3.7.2	Ongoing, simulated phishing exercises and security awareness training for District staff.		
3.7.3	Monitoring for District staff or student-facing credentials appearing in known data-breach or dark-web sources.		
3.7.4	Email archiving sufficient to support public records requests and litigation hold requirements applicable to a Mississippi public school district.		
3.8.1	Vendor must describe how the proposed solution supports the District's obligations under FERPA with respect to student personally identifiable information. (M)		
3.8.2	Vendor must describe data encryption practices for data at rest and in transit.		
3.8.3	Vendor must disclose where covered data is hosted/processed and describe any subcontractor or sub-processor relationships involved in service delivery.		
3.8.4	Vendor must provide evidence of an independent security attestation (e.g., SOC 2 Type II or equivalent) covering the proposed service.		

Exhibit E-1

Other Required Forms

Document 1: Proposal Form and Signature Page

The undersigned proposes to furnish and deliver all items and/or perform all services in accordance with all sections of this RFP, including the Proposal Form, Instructions and Conditions, Specifications, and any Addenda issued.

Company Name: _____

Address: _____

Phone: _____ Email: _____

Authorized Representative (Printed): _____

Signature: _____

Date: _____

Business Classification (circle one):

Woman-Owned Minority-Owned Woman & Minority-Owned Non-Minority

Addendum Acknowledgment:

Addendum No. ____ Date ____ Addendum No. ____ Date ____

Addendum No. ____ Date ____ Addendum No. ____ Date ____

Exhibit E-2

Document 2: Submission Cover Sheet and Configuration Summary

By signing below, the vendor certifies that they are authorized to bind the organization and that the proposal complies with all RFP requirements.

Vendor Name: _____
Authorized Signature: _____
Date: _____

Configuration Summary (100 words or less):
_____
_____
_____
_____
_____

Exhibit E-3

Document 3: Assurances and Signature Form

The vendor certifies compliance with all applicable federal, state, and local laws and regulations, including civil rights, health and safety, confidentiality, and background check requirements.

Organization Name: _____

Authorized Representative (Printed): _____

Signature: _____

Date: _____

Document 4: Independent Contractor Debarment Verification

Registered in SAM.gov: ☐ Yes ☐ No

Registered with Mississippi Secretary of State: ☐ Yes ☐ No

The contractor certifies that neither the organization nor its partners or subcontractors are debarred from doing business with the **federal government or the State of Mississippi.**

Authorized Signature: _____

Date: _____

Bid Proposal: **RFP 2026-02-27**

Bid Title**: Advanced Email and Collaboration Security Solution**

Submission Deadline Date and Time: _____

Participating Vendor Name_____

Address_____

Handwritten Signature_____

Addendums Acknowledge Yes_____ or No _____

If this page is not displayed when the deadline opening date occurs, it will not be acknowledged or allowed to be presented. This applies to all submitted proposals whether mailed, hand delivery or electronically emailed.

End of Bid Document